Mysql的安全设置

我们把mysql安装在/usr/local/mysql目录下，我们必须建立一个用户名为mysql用户组为mysql的用户来运行我们的mysql，同时我们要把它的配置文件拷贝到/etc目录下，

禁止mysql用户远程登陆

如果安装mysql多实例 要以端口号为目录命名并保持路径一致，方便多实例启动脚本启动mysql 多实例安装最好使用mysql的二进制文件来安装

使用用户mysql来启动我们的mysql:

/usr/local/mysql/bin/mysqld\_safe -user=mysql &

（1）修改root用户的密码

如果采用rpm安装 会产生随机密码文件，文件在/root下 隐藏文件.mysql\_secure文件里，到文件里得到密码后删除此文件，登陆到mysql中修改密码。

（2）删除默认的数据库用户

我们的数据库是在本地，并且也只需要本地的php脚本对mysql进行读取，所以很多用户不需要。mysql初始化后会自动生成空用户和test库，这会对数据库构成威胁，我们全部删除。

/usr/local/mysql/bin/mysql\_secure\_installation

（3）改变默认的mysql管理员的用户名

因为默认的mysql的管理员名称是root，所以如果能够修改的话，能够防止一些脚本小子对系统的穷举。我们可以直接修改数据库，把root用户改为"admin"

（4）一高本地安全性

提高本地安全性，主要是防止mysql对本地文件的存取，比如黑客通过mysql把/etc/passwd获取了，会对系统构成威胁。mysql对本地文件的存取是通过SQL语句来实现，主要是通过Load DATA LOCAL INFILE来实现，我们能够通过禁用该功能来防止黑客通过SQL注射等获取系统核心文件。

禁用该功能必须在 my.cnf 的[mysqld]部分加上一个参数：

set-variable=local-infile=0

（5）禁止远程连接mysql

因为我们的mysql只需要本地进行连接，所以我们无需开socket进行监听，那么我们完全可以关闭监听的功能。

有两个方法实现：

配置my.cnf文件，在[mysqld]部分添加 skip-networking 参数

mysqld服务器中参数中添加 --skip-networking 启动参数来使mysql不监听任何TCP/IP连接，增加安全性。

（6）控制数据库访问权限

最好建立一个用户只针对某个库有 update、select、delete、insert、drop table、create table等权限，这样就很好避免了数据库用户名和密码被黑客查看后最小损失。

（7）限制一般用户浏览其他用户数据库

如果有多个数据库，每个数据库有一个用户，那么必须限制用户浏览其他数据库内容，可以在启动MySQL服务器时加--skip-show-database 启动参数就能够达到目的。

（8）忘记mysql密码的解决办法

如果不慎忘记了MySQL的root密码，我们可以在启动MySQL服务器时加上参数--skip-grant-tables来跳过授权表的验证 (./safe\_mysqld --skip-grant-tables &)，这样我们就可以直接登陆MySQL服务器，然后再修改root用户的口令，重启MySQL就可以用新口令登陆了。

（9）数据库文件的安全

我们默认的mysql是安装在/usr/local/mysql目录下的，那么对应的数据库文件就是在/usr/local/mysql/var目录下，那么我们要保证该目录不能让未经授权的用户访问后把数据库打包拷贝走了，所以要限制对该目录的访问。

我们修改该目录的所属用户和组是mysql，同时改变访问权限：

chown -R mysql.mysql /usr/local/mysql/var

chmod -R go-rwx /usr/local/mysql/var

(10) 删除历史记录

执行以上的命令会被shell记录在历史文件里，比如bash会写入用户目录的.bash\_history文件，如果这些文件不慎被读，那么数据库的密码就会泄漏。用户登陆数据库后执行的SQL命令也会被MySQL记录在用户目录的.mysql\_history文件里。如果数据库用户用SQL语句修改了数据库密码，也会因.mysql\_history文件而泄漏。所以我们在shell登陆及备份的时候不要在-p后直接加密码，而是在提示后再输入数据库密码。

另外这两个文件我们也应该不让它记录我们的操作，以防万一。

rm .bash\_history .mysql\_history

cat /dev/null > .bash\_history

cat /dev/null > .mysql\_history

(11) 其他

另外还可以考虑使用chroot等方式来控制mysql的运行目录，更好的控制权限，具体可以参考相关文章。